Chair Cathy McMorris Rodgers
Opening Statement—Subcommittee on Environment, Manufacturing, and Critical Materials:
"Ensuring the Cybersecurity of America's Drinking Water Systems"
January 31, 2024

As prepared for delivery

Good afternoon to my colleagues and our witnesses, and thank you, Chairman Carter.

I look forward to working with you as you lead this subcommittee.

Every day, more and more of our economy and way of life moves online.

Our financial, health, public utilities, and energy systems are all increasingly being operated electronically.

That includes our public drinking water systems.

This shift has significantly enhanced the efficiency of these systems... it has improved water quality, reduced unnecessary expenses, and helped get this vital resource to more Americans.

As our technology becomes more advanced, though, these systems likely will move online more and more...

...making them increasingly vulnerable to cyberattacks by adversaries and other bad actors wishing to do us harm.

It's vital that we take steps to safeguard this key infrastructure from future cyberthreats and work with utility companies and others to mitigate those risks.

Cybercriminals are estimated to have made nearly $8 trillion in 2023—a number that's expected to rise to around $10.5 trillion by next year.

Recent attacks on American drinking water delivery systems by Iran-tied cybercriminals underscore the need for strengthening their cybersecurity.

The targeting of this critical infrastructure puts both our public health and our economy in jeopardy.

The cybersecurity risks to these systems are expected to become increasingly frequent and complex.

From ransomware threats, where a bad actor's attack compromises internal, administrative information like customers' personal information….
...to criminals potentially gaining control of a drinking water system in order to compromise the quality of the water being sent out to customers.

The implications of these attacks go far beyond our water systems...

...compromising them could prevent doctors from carrying out medical procedures at hospitals, disrupt the delivery of electricity, or shut down altogether emergency services, like firefighting operations.

These are not acceptable outcomes.

Today will be an opportunity to hear from experienced and well-positioned stakeholders in order to better understand the threats as well as how we can most effectively address them.

It is important that we strike the right balance for local utilities as they take steps to improve the cyber-resiliency of their facilities...

...including, ensuring the federal government isn't getting in the way of those efforts to make progress.

Current law mandates that, every five years, drinking water systems serving more than 3,330 people assess their vulnerabilities to attacks.

...and that they incorporate the findings of these assessments into their emergency response plans.

This ensures water facility operators are better prepared to mitigate threats...

...while also protecting them from cumbersome and ill-suited regulations that could hinder their ability to quickly respond when threats do arise.

While there is always room for improvement, granting the federal government sweeping cybersecurity authorities over this sector—as some have suggested—will do more harm than good.

A one-sized fits all approach for the 50,000 unique drinking water utilities around the country is unworkable…

…and the federal rulemaking process is problematic…

…it is protracted and cumbersome…it fails to foster collaboration…and it advertises to adversaries the very systems intruders will need to target with cyberattacks.

Federal agencies play an important role in the overall cyber-resiliency of our water systems.

...and the Environmental Protection Agency, as the federal expert in drinking and wastewater, is the one best suited to serve as the lead in managing risk in this sector...
...EPA and others play important roles, whether that's facilitating education and outreach with operators, or providing technical assistance.

That said, the EPA should not be in the business of micromanaging water utilities or dictating how they maintain and operate their online systems.

Today's conversation will be an opportunity to explore the non-regulatory resources that the EPA and others already offer to the water sector…

…like the Water ISAC, which is an all-threats information sharing source for water utilities...

…or the Cyber Readiness Institute, which works with companies to empower smaller water systems with free tools and resources to help them become more secure and resilient.

Resources like these can help water systems, without the in-house expertise, better implement cyber practices.

In order to protect people and this critical infrastructure...

...we must ensure water facility operators are able to innovate and adapt to evolving cyber threats and protect the systems they oversee.

I look forward to today's hearing and discussing how we will enhance our cybersecurity to protect this infrastructure, which is so vital for the livelihoods of Americans' lives.

I yield back.